UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF WISCONSIN

UNITED STATES OF AMERICA,

Plaintiff,

Case No. 17-CR-124

v.

MARCUS HUTCHINS,

Defendant.

DEFENDANT'S MOTION TO DISMISS THE FIRST SUPERSEDING INDICTMENT (FAILURE TO STATE OFFENSES AND MULTIPLICITY) [REPLACING DKT. NO. 56]

Defendant Marcus Hutchins seeks dismissal of Counts One through Eight and Ten of the first superseding indictment for their failure to state offenses and for multiplicity. Fed. R. Crim. P. 12(b)(3)(A)(v). The Court should dismiss these counts against Mr. Hutchins with prejudice.

Counts One and Seven allege a conspiracy and attempt to violate the Computer Fraud and Abuse Act, 18 U.S.C. § 1030(a)(5)(A). Those counts should be dismissed because the superseding indictment fails to allege any facts that would show Mr. Hutchins had any intent to cause "damage" to a protected computer within the meaning of the statute.

Counts One through Six allege violations of the Wiretap Act, 18 U.S.C. §§ 2511 and 2512. Those counts fail to state an offense because software such as Kronos and UPAS Kit is not an "electronic, mechanical, or other device" as defined by the Wiretap Act. Count Three should also be dismissed because it is multiplicitous of Count Two.

Finally, Counts One, Four through Eight, and Ten should be dismissed because the government does not allege the necessary intent and causation to state those offenses.

BACKGROUND

This case stems from the alleged development and sale of two types of malicious software: UPAS Kit and Kronos. Mr. Hutchins was indicted on July 12, 2017 on six counts alleging violations of the Computer Fraud and Abuse Act (CFAA) and the Wiretap Act. (Dkt. No. 6.) The government filed a first superseding indictment on June 5, 2018. (Dkt. No. 86.)[1]

[1] The first superseding indictment includes new factual allegations, substantially broadens Count One, and adds four new counts. Specifically, Count One charges Mr. Hutchins with conspiring to violate the CFAA and Wiretap Act. Counts Two and Three charge Mr. Hutchins with advertising and aiding and abetting the advertisement of an electronic communication interception device in violation of the Wiretap Act. Counts Four and Five allege that Mr. Hutchins aided and abetted another person in sending and selling an electronic communication interception device in violation of the Wiretap Act. Count Six charges that Mr. Hutchins endeavored to intercept and procured another person to intercept electronic communications in violation of the Wiretap Act. Count Seven alleges that Mr. Hutchins caused and aided and abetted another in attempting to cause damage to a computer without authorization in violation of the CFAA. Count Eight charges that Mr. Hutchins aided and abetted another to access a computer without authorization in violation of the CFAA. Count Nine alleges that Mr. Hutchins made a false statement to the FBI in violation of 18 U.S.C. § 1001. Finally, Count Ten claims that Mr. Hutchins conspired to engage in wire fraud in violation of 18 U.S.C. § 1343.

***

The defense has concurrently filed two other separate motions to dismiss the first superseding indictment. The first seeks dismissal on extraterritoriality grounds. The second seeks dismissal of a count that mis-describes the mental state required by the statute at issue. This motion focuses on the first superseding indictment's failure to state offenses and multiplicitous charges.

This motion to dismiss replaces the one the defense filed on March 30, 2018, Dkt. No. 56. The government filed a response on April 18, 2018, Dkt. No. 65, and the defense filed a reply on April 30, 2018, Dkt. No. 71. Per the Court's June 22, 2018 order, those filings should be stricken and not considered. (Dkt. No. 91 at 2.)

LEGAL STANDARD

A valid indictment "must allege that the defendant performed acts which, if proven, constituted a violation of the law that he is charged with violating." *United States v. Gimbel*, 830 F.2d 621, 624 (7th Cir. 1987). A defendant may raise the government's failure to state an offense before trial "if the basis for the motion is reasonably available and the motion can be determined without a trial on the merits." Fed. R. Crim. P. 12(b)(3)(B)(v). A court must dismiss the indictment when the allegations in the indictment fail to state an offense. *United States v. Risk*, 843 F.2d 1059, 1060 (7th Cir. 1988). In other words, when the

government's "characterization of the undisputed facts [does] not constitute a violation of any statute," there is "no case to prove" and so charges may properly be dismissed before any trial. *Id*.

ARGUMENT

The first superseding indictment fails to allege acts by Mr. Hutchins which, if proven, would constitute violations of law. Because there is "no case to prove," the Court should dismiss Counts One, Three, and Eight through Ten.

1. Counts One and Seven Do Not Allege Violations of the Computer Fraud and Abuse Act, 18 U.S.C. § 1030(a)(5)(A)

Counts One and Seven allege that Mr. Hutchins conspired, aided and abetted, and directly committed a violation of 18 U.S.C. § 1030(a)(5)(A). This section prohibits "knowingly caus[ing] the transmission of a program, information, code, or command, and as a result of such conduct, intentionally caus[ing] damage without authorization, to a protected computer." "Damage," in turn, is defined as "any impairment to the availability or integrity of data, a program, a system, or information." 18 U.S.C. § 1030(e)(8).

In spite of this specific definition, the first superseding indictment claims only that Kronos "recorded and exfiltrated user credentials and personal identifying information from protected computers," (First Superseding Indictment ¶ 1(e)), and that UPAS Kit "allowed for the unauthorized exfiltration of information from protected computers" (*id*. ¶ 1(f)). Nothing in these

descriptions indicates that Mr. Hutchins (or Individual A, for that matter) agreed or attempted to intentionally cause "impairment to the availability or integrity" of anything. He is alleged only to have "recorded and exfiltrated" data—that is, making a copy of the data and taking it away.

These actions alone do not constitute damage within the meaning of the CFAA: they do not affect the "availability" or "integrity" of the underlying data.

The Seventh Circuit has repeatedly found that "damage" requires more than what the indictment here alleges. On one end of the spectrum, in *Int'l Airport Ctrs. LLC v. Citrin*, a defendant was found to have caused damage when he installed software on his employer's computer that permanently deleted stored files. 440 F.3d 418, 419 (7th Cir. 2006). And in *United States v. Mitra*, a defendant's disruption of the functionality of Madison's emergency response system caused damage within the meaning of the CFAA. 405 F.3d 492, 494-95 (7th Cir. 2005).

On the other end of the spectrum is *Fidlar Technologies v. LPS Real Estate Data Solutions, Inc.*, 810 F.3d 1075 (7th Cir. 2016). There, a data analytics company was accused of violating § 1030(a)(5)(A) when it used a computer program to download real estate records in bulk from county databases in violation of a technology provider's license agreement. *Id.* at 1078. The Seventh Circuit found that the company did not cause damage within the meaning of the CFAA because it did not "alter or disrupt" the technology provider's service—it

simply downloaded information while avoiding the provider's attempts to track user activity. *Id.* at 1084.

The first superseding indictment's allegations here are on the *Fidlar Technologies* end of the scale. Indeed, as Judge Stadtmueller has noted, "merely accessing and disseminating information" on a computer does not meet the CFAA's "very specific" definition of damage—and any claim otherwise "borders on the frivolous." *Landmark Credit Union v. Doberstein*, 746 F. Supp. 2d 990, 993-94 (E.D. Wis. 2010).

The first superseding indictment does not allege that Kronos or UPAS Kit "impaired the availability or integrity" of data, a program, a system, or information in any way. For this reason alone, it fails to state an offense in Counts One and Seven, and they must be dismissed.

2. Counts One Through Six Do Not Allege Violations of the Wiretap Act

Counts One through Six allege that Mr. Hutchins violated the Wiretap Act in various ways. Counts Two and Three allege Mr. Hutchins advertised and promoted an "electronic, mechanical, or other device" for surreptitious interception—specifically, the Kronos software—in violation of 18 U.S.C. §§ 2512(1)(c)(i) and (ii). Counts Four and Five claim that Mr. Hutchins aided and abetted Individual A's sending and sale of an "electronic, mechanical, or other device" that is primarily useful for surreptitious interception. And Counts One and Six allege that Mr. Hutchins conspired to violate and violated 18 U.S.C. §

2511 by endeavoring to intercept and procuring another person to intercept and endeavor to intercept electronic communications. Per 18 U.S.C. § 2510(4), an interception can only be accomplished via an "electronic, mechanical, or other device." Thus, the existence of an "electronic, mechanical, or other device" is a critically important element of every charge alleging a violation of the Wiretap Act. But neither Kronos nor UPAS Kit is such a device.

At 18 U.S.C. § 2510(5), the Wiretap Act specifically defines the term "electronic, mechanical, or other device" to mean "any device or apparatus which can be used to intercept a wire, oral, or electronic communication," with some exceptions not relevant in this case. While § 2510 does not specifically define the word "device," undefined terms in a statute are deemed to have their ordinary meaning. *Taniguchi v. Kan Pacific Saipan, Ltd.*, 566 U.S. 560, 566 (2012).

The Merriam-Webster Dictionary defines "device" to mean, *inter alia*, "a piece of equipment or a mechanism designed to serve a special purpose or perform a special function."[2] It offers as an example of usage for this definition "a hidden recording device"—precisely the type of instrument at the heart of the Wiretap Act's prohibitions. A software program is neither a "piece of equipment" nor a "mechanism." Thus, it does not meet the ordinarily understood meaning of "device."

[2] https://www.merriam-webster.com/dictionary/device (last visited July 13, 2018).

Returning to the first superseding indictment, Counts Two through Five claim that Mr. Hutchins advertised, sent, and sold the Kronos software. But these four § 2512 counts cannot survive where the charges are based on advertising, sending, and selling software. Section 2512 makes it illegal only to advertise, send, or sell an "electronic, mechanical, or other device" that is primarily useful for surreptitious interception or promoted as such. Once again, software is not a device because it is not an "apparatus," a "piece of equipment" or a "mechanism." It is a computer program.

The Seventh Circuit has recognized this important distinction. In a wiretapping case involving the use of software to intercept a communication, the Court determined that the *computers running software* were the relevant devices for purposes of the offense—it did not focus on the software installed on the devices. *United States v. Szymuszkiewicz*, 622 F.3d 701, 707 (7th Cir. 2010) (as amended Nov. 29, 2010).

The Seventh Circuit is not the only court to take this approach. In *Potter v. Havlicek*, 2008 WL 2556723 (S.D. Ohio 2008), a civil case alleging a violation of § 2512, the plaintiff argued that the defendant made and sold surveillance software called "Activity Monitor." The district court there found that the software was not a device for purposes of § 2512:

> Section 2512 makes the manufacture and/or trafficking of "any electronic, mechanical, or other device" illegal. The phrase "electronic, mechanical, or other device" is defined in 18 U.S.C. §

> 2510(5) to generally mean "any device or apparatus which can be used to intercept a wire, oral, or electronic communication . . . ." Clearly, Activity Monitor alone cannot be used to intercept communications. *It must be installed in a device, such as a computer, to be able to do so.*

Id. at *8 (emphasis added).

Counts One and Six fail for a similar reason. The first superseding indictment alleges that Mr. Hutchins conspired to violate and violated 18 U.S.C. § 2511 by endeavoring to intercept, procuring another person to intercept and endeavor to intercept "certain electronic communications, namely computer keystrokes[.]" The Wiretap Act defines "intercept" to mean "the aural or other acquisition of the contents of any wire, electronic, or oral communication through the use of any *electronic, mechanical, or other device*." 18 U.S.C. § 2510(4) (emphasis added). There can be no interception within the meaning of the statute if there is no "electronic, mechanical, or other device." And, as explained above, UPAS Kit and Kronos are not.

For these reasons, Counts One through Six must be dismissed for their failure to state an offense.

3. Counts Two and Three are Multiplicitous and Expose Mr. Hutchins to Double Jeopardy

Count Three should be dismissed for an additional reason: it charges the same offense as Count Two. Together, then, they "charge a single offense as separate counts," which is a problem of multiplicity, one that "exposes a

defendant to the threat of receiving multiple punishments for the same offense in violation of the Double Jeopardy Clause of the Fifth Amendment." *United States v. Ajayi*, 808 F.3d 1113, 1123 (7th Cir. 2015), citing *United States v. Starks*, 472 F.3d 466, 468-69 (7th Cir. 2006).

To determine whether counts are multiplicitous, the Court "look[s] to the applicable criminal statute to see what the allowable 'unit' of prosecution is—the minimum amount of activity for which criminal liability attaches." *Ajayi*, 808 F.3d at 1123, quoting *United States v. Allender*, 62 F.3d 909, 912 (7th Cir. 1995). Under the *Blockberger* test, "[t]he applicable rule is that where the same act or transaction constitutes a violation of two distinct statutory provisions, the test to be applied to determine whether there are two offenses or only one, is that each provision requires proof of an additional fact which the other does not." *Blockberger v. United States*, 284 U.S. 299, 304 (1932).

The structure of § 2512 shows that Congress did not intend subsections (1)(c)(i) and (1)(c)(ii) to both be charged for the same conduct. The statute includes distinct provisions to punish (a) sending, (b) manufacturing, assembling, possessing or selling, and (c) advertising an electronic, mechanical, or other device primarily useful for surreptitious interception. 18 U.S.C. § 2512(1)(a), (b), & (c). Unlike subsections (1)(a) and (1)(b), Congress drafted § 2512(1)(c) to include two separate provisions separated by the disjunctive "or," which are identical except for a single element. Specifically, § 2512(1)(c)(i)

punishes the advertisement of an interception device when one *knows or has reason to know that the design of the device renders it primarily useful for the purpose of surreptitious interception*. And § 2512(1)(c)(ii) punishes the advertisement of an interception device in a manner that *promotes its use for the purpose of surreptitious interception*.

As applied to Mr. Hutchins, §§ 2512(1)(c)(i) and (ii) do not each require proof of an additional fact which the other does not. If one advertises a device that is designed for surreptitious interception, he necessarily promotes its use for surreptitious interception. Congress did not intend for both prongs of § 2512(1)(c) to penalize a single act. Thus, Count Three must be dismissed.

4. Counts One, Four through Eight, and Ten Do Not Allege the Requisite Intent and Causation to Make Out Viable Claims

Finally, the superseding indictment does not allege the necessary intent and causation to state Counts One, Four through Eight, and Ten. Whether the government's theory is direct liability, conspiracy, attempt, or aiding and abetting, each requires that the government allege (and ultimately prove beyond a reasonable doubt) that Mr. Hutchins specifically intended a violation of the underlying substantive law to occur. *7th Circuit Pattern Jury Instructions* at 4.09, 5.06 & 5.09 (2012 ed.); *United States v. Garcia*, 45 F.3d 196, 199 (7th Cir. 1995). The first superseding indictment's allegations do not support that conclusion.

With respect to Mr. Hutchins and Individual A's alleged distribution of UPAS Kit and Kronos, the government conflates their alleged *selling* of the software with a *specific intent* for buyers to commit an illegal act with the software. There is no allegation that Mr. Hutchins or Individual A intended any specific result to occur because of the sales. There is no claim that they intended for the buyers to do anything in particular with the program. The first superseding indictment simply alleges an intent to give the software to a paying customer. Merely writing a program and selling it—when any illegal activity is up to the buyer to perform—is not enough to allege specific intent by Mr. Hutchins.

As the Seventh Circuit has made clear in the context of drug-distribution cases, a buyer-seller relationship—without more—does not establish a conspiracy. *United States v. Johnson*, 592 F.3d 749, 759 (7th Cir. 2010). There must be an agreement "to commit a crime *other than* the crime that consists of the sale itself." *Id.* (emphasis in original) (citations omitted). To form a conspiracy, the seller must not only know that the buyer will re-sell the drugs—the buyer must *intend* for it to happen. *7th Cir. Criminal Pattern Jury Instruction* 5.10.

Likewise, there is no viable liability where the government merely alleges that Mr. Hutchins and Individual A sold Kronos or UPAS Kit to a buyer—even if they knew the buyer could later use it to cause damage to a computer, intercept a communication, or access a computer without authorization. The first

superseding indictment must *also* establish that Mr. Hutchins and his co-conspirator specifically *intended* for the buyer to commit those acts. For Mr. Hutchins to be guilty of the charged conspiracy, his and his co-conspirator's goal—their conspiratorial objective—must have been for those substantive crimes to occur. But this is not alleged in the indictment.

Nor do the first superseding indictment's new allegations involving Individual B establish intent or causation on Mr. Hutchins' part. The superseding indictment claims that Mr. Hutchins distributed Kronos to Individual B, and that he knew Individual B "was involved in the various cyber-based criminal enterprises including the unauthorized access of point-of-sale systems and the unauthorized access of ATMs." (First Superseding Indictment ¶ 4(j).) But it does not allege that Mr. Hutchins specifically *intended* for Individual B to use Kronos to gain unauthorized access to computers (nor that any such thing actually occurred).[3]

[3] One of the government's new allegations deserves a special mention. The superseding indictment states that Mr. Hutchins "hacked control panels" associated with a so-called competing malware called Phase Bot and wrote a blog post about it. (First Superseding Indictment ¶ 4(h).) It does not appear that this allegation alone is the basis of any count, as Mr. Hutchins would presumably be charged with a direct—rather than inchoate—violation of § 1030(a)(2)(C) if that were the case. To the extent it is a basis for any count, however, the defense notes that analyzing malware is, in fact, what Mr. Hutchins does professionally. In total, Mr. Hutchins wrote a total of three lengthy blog posts to educate the public about Phase Bot's structure and functionality. These blog posts were based on Mr. Hutchins' analysis of Phase Bot installed on his own computers. Any attempt to punish or interfere with Mr. Hutchins' lawful security research and publishing activities would, of course, violate his First Amendment rights.

For these reasons, Counts One, Four through Eight, and Ten do not state offenses.

CONCLUSION

The allegations in the first superseding indictment do not establish Mr. Hutchins' commission of the offenses charged in Counts One through Eight and Ten. They must be dismissed with prejudice.

DATED: July 13, 2018

Respectfully submitted,

/s/ Marcia Hofmann
MARCIA HOFMANN
Zeitgeist Law PC
25 Taylor Street
San Francisco, CA 94102
Email: marcia@zeitgeist.law
Telephone: (415) 830-6664

/s/ Brian E. Klein
BRIAN E. KLEIN
Baker Marquart LLP
2029 Century Park E – Suite 1600
Los Angeles, CA 90067
Email: bklein@bakermarquart.com
Telephone: (424) 652-7800

/s/ Daniel W. Stiller
DANIEL W. STILLER
DStillerLLC
Box 511130
Milwaukee, WI 53203
Email: dan@dstillerllc.com
Telephone: (414) 207-3190

Attorneys for Marcus Hutchins